

Amendment to the Claims

Applicant respectfully requests the following amendments to the claim set:

1. (Currently Amended) A control device for authenticating the identification of a user prior to access to a software application, the control device comprising:

- a) a biometric signal acquisition module located on a computer input device;
- b) an area on the computer input device through which the biometric acquisition module may obtain the biometric signal of a user in control of the computer input device; and
- c) a software interface for comparing the acquired biometric signal to a collection of authorized signals to determine if the individual controlling the computer input device is authorized to access a software application, wherein the only identification required is the biometric signal.

2. (Currently Amended) A method for preventing access to a software application the method comprising the steps of: (a) obtaining a base line biometric signal from an authorized user; (b) obtaining through a biometric acquisition module located in a computer input device a current biometric signal from the individual controlling the computer input device to obtain access to software, wherein the only identification required is the biometric signal; (c) comparing the current biometric signal with the baseline biometric signal to determine whether the user is authorized to access the software; and (d) allowing access to the software if the comparison reveals that the current user is authorized to access the software.

3. (Currently Amended) A method for providing security to a network of computers, the method comprising of steps of (a) obtaining base line biometric signals for all authorized users of a network; (b) providing a biometric acquisition device in a computer input device operated by the hand of a user at the location of each of the authorized users; (c) obtaining a current biometric signal through the computer input device from an individual attempting to access the network, wherein the only identification required is the biometric signal; (d) comparing the current biometric signal with the stored baseline biometric signal to determine whether the current user is authorized to access the network; and (e) allowing access to the network if the user is authorized.

4. (Original) The method set forth in the claim 3 above further comprising the step of denying access to the network if the current user is not authorized.

5. (Original) The method set forth in the claim 3 above further comprising the step of storing the biometric from an unauthorized user attempting to access the network and providing that biometric to the manager of the network.

6. (New) The control device set forth in the claim 1 above, wherein the software interface also performs multiple authentication processes, even during use of the software application or other software applications, to determine if the individual presently controlling the computer input device is still authorized to access the software application.

7. (New) The method set forth in the claim 2 above further comprising the step of (e) performing multiple authentication processes, even during the use of the software application or other software applications, to determine if the individual presently controlling the computer input device is still authorized to access the software application.

8. (New) The method set forth in the claim 3 above further comprising the step of (f) performing multiple authentication processes, even during the use of the network, to determine if the individual presently controlling the computer input device is still authorized to access the network.